WHAT IS CLAIMED IS:

1   1. A method for communication of messages in a secure manner in a

2 communication environment which is subject to compromise, the method comprising:

3   *a.* providing an escrow agent, wherein said escrow agent generates a pair of keys

4 comprising a public key and a private key; *OK*

5   *b.* causing said escrow agent to communicate said public key to all parties within

6 a communication system to be used to support secure communication; *OK*

7   *c.* extracting at each party a common benchmark; *make argument*

8   *d.* agreeing among each party on a starting interval key referenced to said *make argument.*

9 common benchmark;

10   *e.* causing each party to generate iteratively a next interval key independently of *Step E*

11 each other party but with reference to an interval index, wherein said interval key is

12 encrypted by said public key; thereafter

13   *f.* initiating a secure communication between or among parties using reference to

14 said interval index and without communicating or exchanging their respective interval keys;

15   *g.* causing each party to a secure communication to encrypt a message to be *Step J*

16 secured using the common interval key independently computed based on said common

17 interval index; and

18   *h.* causing said encrypted message to be communicated within said system such

19 that said encrypted message can be decrypted using said common interval key.

1   2. The method according to claim 1 wherein said parties exchange their

2 respective interval indexes and wherein the parties with the older interval indexes advance *Step I*

3 their interval index and compute said interval key corresponding to the latest interval index.

synchronously.
one way of
making an agreement.

1   3. The method according to claim 2 wherein each party destroys each

2 prior interval key after a new interval key is generated so that an older interval key cannot be

3 recovered.

1   4. The method according to claim 1 wherein said interval index is not

2 communicated to said escrow agent.

1   5. The method according to claim 1 wherein said starting interval key is
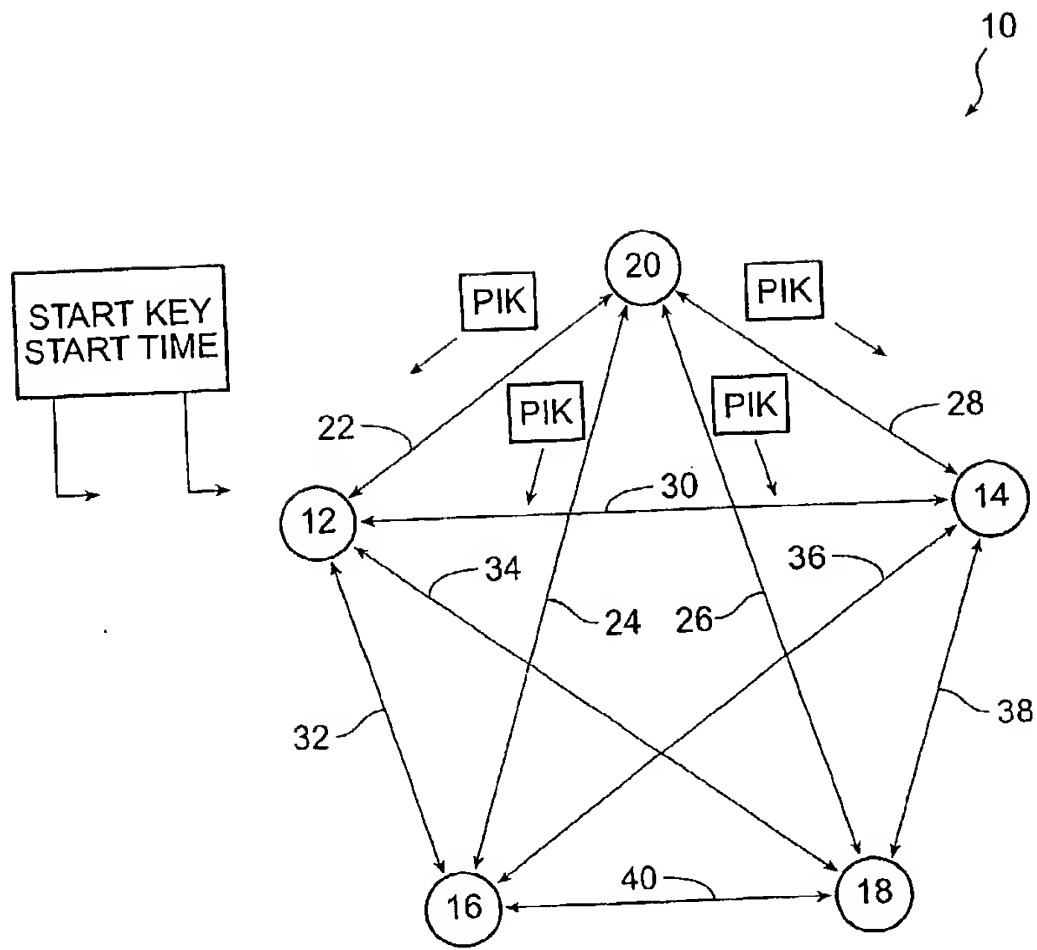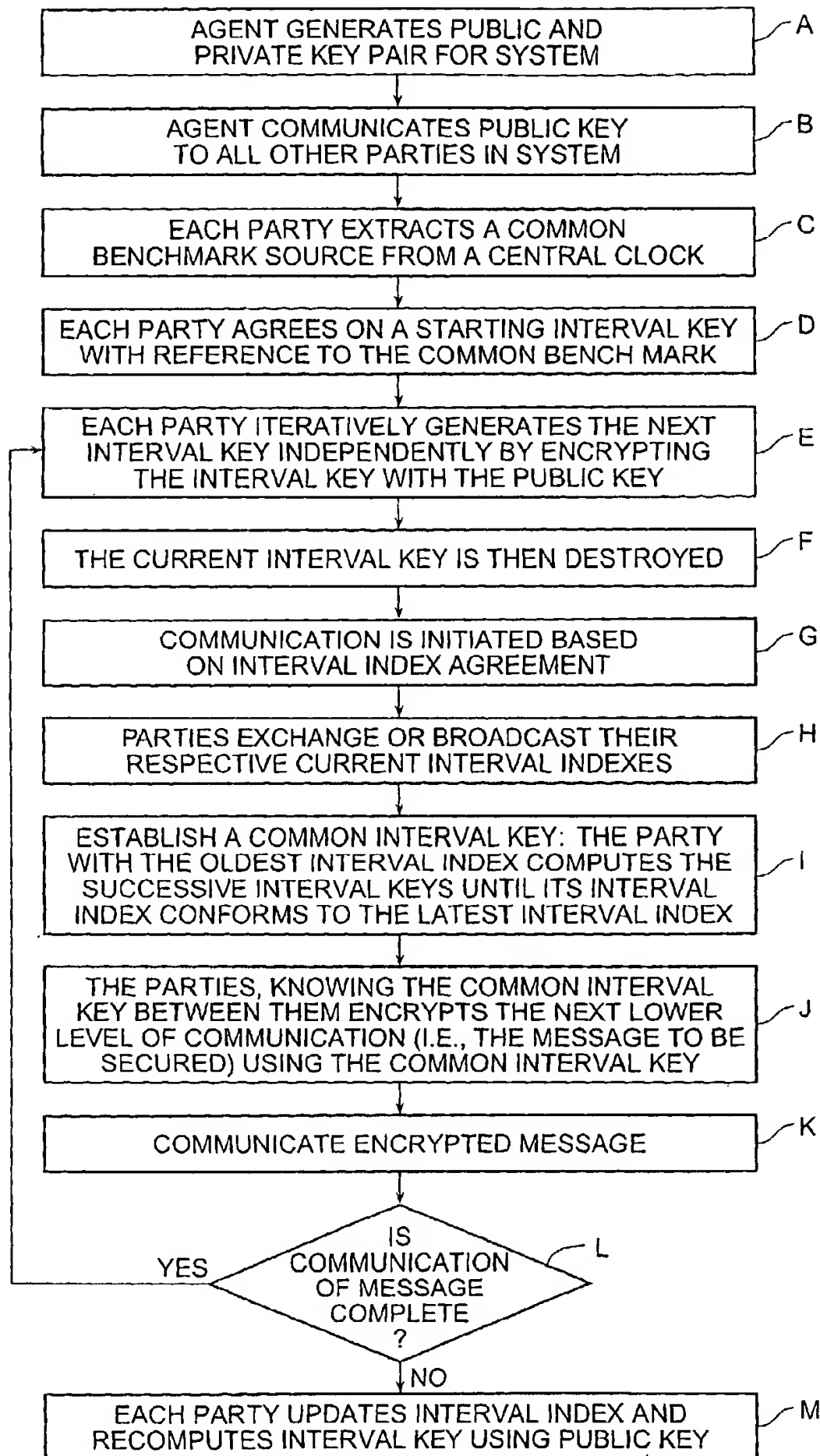
2 not communicated to said escrow agent.

8

10

FIG. 1

```
┌──────────────────────────────────────┐
│   AGENT GENERATES PUBLIC AND         │──A
│   PRIVATE KEY PAIR FOR SYSTEM        │
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   AGENT COMMUNICATES PUBLIC KEY      │──B
│   TO ALL OTHER PARTIES IN SYSTEM     │
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   EACH PARTY EXTRACTS A COMMON       │──C
│   BENCHMARK SOURCE FROM A CENTRAL CLOCK│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   EACH PARTY AGREES ON A STARTING INTERVAL KEY│──D
│   WITH REFERENCE TO THE COMMON BENCH MARK│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   EACH PARTY ITERATIVELY GENERATES THE NEXT│──E
│   INTERVAL KEY INDEPENDENTLY BY ENCRYPTING│
│   THE INTERVAL KEY WITH THE PUBLIC KEY│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   THE CURRENT INTERVAL KEY IS THEN DESTROYED│──F
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   COMMUNICATION IS INITIATED BASED   │──G
│   ON INTERVAL INDEX AGREEMENT        │
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   PARTIES EXCHANGE OR BROADCAST THEIR│──H  (not interval keys)
│   RESPECTIVE CURRENT INTERVAL INDEXES│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   ESTABLISH A COMMON INTERVAL KEY: THE PARTY│──I
│   WITH THE OLDEST INTERVAL INDEX COMPUTES THE│
│   SUCCESSIVE INTERVAL KEYS UNTIL ITS INTERVAL│
│   INDEX CONFORMS TO THE LATEST INTERVAL INDEX│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   THE PARTIES, KNOWING THE COMMON INTERVAL│──J
│   KEY BETWEEN THEM ENCRYPTS THE NEXT LOWER│
│   LEVEL OF COMMUNICATION (I.E., THE MESSAGE TO BE│
│   SECURED) USING THE COMMON INTERVAL KEY│
└──────────────────────────────────────┘
                  │
┌──────────────────────────────────────┐
│   COMMUNICATE ENCRYPTED MESSAGE      │──K
└──────────────────────────────────────┘
                  │
              ╱ IS ╲
        YES ╱ COMMUNICATION ╲ ──L
           ╲ OF MESSAGE ╱
            ╲ COMPLETE ╱
               ╲ ? ╱
                │ NO
┌──────────────────────────────────────┐
│   EACH PARTY UPDATES INTERVAL INDEX AND│──M
│   RECOMPUTES INTERVAL KEY USING PUBLIC KEY│
└──────────────────────────────────────┘
```

FIG. 2